Zeszyty Naukowe SGSP 2020, Nr 73/1/2020

Grzegorz Matuszek, PhD
WSB University in Dąbrowa Górnicza

DOI: 10.5604/01.3001.0014.0784

CCTV Systems – Technological and Legal Aspects. The Present and the Prospects for Future

Abstract

CCTV system is currently one of the most commonly used means of influencing the safety and public order. A necessary condition for taking full advantage of the system is following technical standards in the process of creating and using CCTV. The current standard for technical standards is PN-EN 62676-1-1: 2014-06 CCTV Surveillance systems used in security. Part 1-1: system requirements – General provisions. The dynamic development of information technologies, including those based on artificial Intelligence, offers a wide range of possibilities. Systems based on advanced software allow automatic notification of threats. This in turn enables limiting the number of employees as well as increasing the efficiency of CCTV. An example of a system based on such software is the Intelligent System of Monitoring and Analysis in Katowice.

Keywords: safety, public order, video monitoring, city monitoring, technical standards, artificial intelligence

Received: 31.01.2020; Reviewed: 07.03.2020; Accepted: 13.03.2020

Monitoring wizyjny – ujęcie prawne i technologiczne. Współczesność i perspektywy

Abstrakt

Monitoringi wizyjne są obecnie jednymi z najszerzej wykorzystywanych środków mających wpływać na bezpieczeństwo i porządek publiczny. Warunkiem pełnego wykorzystania możliwości monitoringu wizyjnego jest przestrzeganie norm technicznych na etapie budowy i eksploatacji systemu. Obecnie aspekty techniczne reguluje norma PN-EN 62676-1-1:2014-06 Systemy dozorowe CCTV stosowane w zabezpieczeniach – Część 1-1: Wymagania systemowe – Postanowienia ogólne. Dynamiczny rozwój technologii informatycznych, w tym opartych na sztucznej inteligencji daje coraz większe możliwości. Systemy wykorzystujące zaawansowane oprogramowanie pozwalają na automatyczne sygnalizowanie zagrożeń. Daje to możliwość ograniczenia personelu oraz zwiększenie skuteczności monitoringów wizyjnych. Przykładem systemu opartego na tego typu oprogramowaniu jest Katowicki Inteligentny System Monitoringu i Analiz.

Słowa kluczowe: bezpieczeństwo i porządek publiczny, monitoring miejski, monitoring wizyjny, normy techniczne, sztuczna inteligencja

Przyjęty: 31.01.2020; Zrecenzowany: 07.03.2020; Zatwierdzony: 13.03.2020

Відеомоніторинг – правовий та технологічний підхід. Сучасність та перспективи

Анотація

На даний момент відеомоніторинг є одним із найбільш широко застосовуваних заходів щодо впливу на громадську безпеку та порядок. Умовою повного використання можливостей відеомоніторингу є відповідність технічним стандартам на етапі побудови та експлуатації системи. В даний час технічні аспекти регулюються нормами PN-EN 62676-1-1:2014-06 Системи спостереження CCTV, що використовуються в забезпеченнях – Частина 1-1: Системні вимоги – Загальні положення. Динамічний розвиток інформаційних технологій, у тому числі на основі штучного інтелекту, дає все більші можливості. Системи, що використовують вдосконалене програмне забезпечення, дозволяють автоматично сигналізувати про загрози. Це дає можливість скоротити персонал та підвищити ефективність відеоспостереження. Прикладом системи на основі цього типу програмного забезпечення є Інтелектуальна Система Моніторингу та Аналізу в м. Катовіце.

Ключові слова: громадський порядок та безпека, моніторинг міста, відеомоніторинг, технічні норми, штучний інтелект

Прийнятий: 31.01.2020; Рецензованої: 07.03.2020; Затверджений: 13.03.2020

Introduction

One of the most important needs of humans is the need for security. It is one of the elements in the hierarchy of needs, which constitute a natural development path of humans, and allows satisfying the basic needs to needs of a higher order [1, pp. 445–446]. Care for security has always accompanied people, it still does and always will [2, p. 291]. The need for security is strongly correlated with the group of physiological needs, which proves that one of the elementary purposes of functioning of an individual is assuring to oneself safe living and conditions for development [3, p. 23]. One of the contemporary methods used for security is the dynamically evolving video surveillance.

Surveillance cameras have become a natural element of our lives. In literature a justified thesis has appeared suggesting that we are living in a monitored society [4, s. 8]. Monitoring has currently become one of the most popular and most widely used means, which is meant to improve the feeling of security [5, p. 30]. The scale of the use of surveillance worldwide may be proven by British research. Practically in all British towns video monitoring systems have been installed, which are still being developed. Already in 2002 in Great Britain there were over 4 million installed cameras which indicates there was one camera per 14 persons [5, p. 36]. Presently the biggest number of monitoring cameras is used in China, where there are over 200 million cameras [6]. In Poland video monitoring including urban monitoring, is also in widespread use. This concerns all provincial towns and more than 85% of county towns [7, p. 8]. One of the causes in a dynamic increase of the use of video monitoring in the system of public security is technical development. The currently used systems are more effective, more precise than those that had been in use only a few years ago. Increasingly frequently they are furnished with computer software that enables automatic identification of vehicle licence plates, identification of anomalies in the monitored place and also identification of images of people.

The objective of the present paper is to present video monitoring as a tool used to enhance public security and order. The author describes CCTV systems in the context of standardisation regulations, which regulate their structure and functioning. It cites standards, the implementation of which assures effective usage of video monitoring. As an example of a system built and used on the basis of binding applicable standardisation regulations it points to the Katowicki Inteligentny System Monitoringu i Analiz (the Katowice Intelligent Monitoring and Analyses System). Another goal of the author is also to indicate and flag possible directions for the development of video monitoring systems. As an example he mentioned the method of machine learning which is one of the most important spheres of artificial intelligence. As regards possible development conditions of CCTV systems, the author invites the reader to deepen his knowledge.

1. Concept of video monitoring

In Poland there is no single recognised definition of video monitoring. Other names concurrently used are video monitoring, video surveillance system, closed-circuit television system or CCTV. Similarly as M. Szumańska, the author is of the opinion that none of those expressions is free of defects [8, p. 11]. The most equivocal and simultaneously the most popular one is "monitoring". It is a simple transposition of the English verb *monitor* which means directly "control" or "listen" [9, p. 117]. This concept is translated accordingly in the "Słownik współczesnego języka polskiego" (Dictionary of contemporary Polish language), i.e. monitoring understood as "[…] execution of permanent observations, carrying out continuous systematic measurements" [10, p. 533]. In literature attempts have been made at defining the concept of video monitoring, taking into account the goal and ways in which the system operates. The goal of operation is indicated among others by P. Kałużny, who describes closed-circuit television as sets of television technical and programme means designated for observation, detection, recording and signalling of conditions pointing to the existence of a hazard of damage or threat to the people and property [11, p. 11]. A definition oriented at the method of operation is presented by P. Waszkiewicz. In his opinion video monitoring (*closed circuit television* – CCTV, German: *Videoüberwachung*) is a system which allows remote observations of events recorded by one camera, and in some cases even as many as a few hundred cameras simultaneously. The system comprises cameras, from which the image is transmitted to the central control rooms where staff may observe the recorded footage on monitors. Video monitoring, also closed-circuit surveillance, differs from common television by the fact that footage from cameras is sent and received only in the central control room, and not in an unlimited number of receivers [5, p. 30]. There is a lack of a statutory definition for video monitoring. The definition of monitoring devised on the basis of "Słownik wyrazów obcych" (Dictionary of foreign words) is presented by the Najwyższa Izba Kontroli (The Supreme Chamber of Control) in information concerning results of inspection of "Functioning of urban video surveillance". According to this definition monitoring is a system of long-term or repeatable observation of a given type of phenomena or response to such phenomena, size, parameters, set properties etc.; it is commonly called watching images on monitors transmitted from a given location with the use of cameras installed there and appropriate lines (also called video monitoring) [8]. With this definition corresponds the one presented by A. Ordysińska. She defines video surveillance as an information transmitting system that consists of planned (continuous method, executed in a specific way with the use of functional guidelines and procedure) observations (frequently also recording) of diverse events that take place in the determined place using technical means, with the aim of preventing crimes, offences, accidents and assignment of fault, responsibility for the committed acts [12, p. 38]. P. Wittich cites a definition of video monitoring systems specified in Polish standard PN-EN 50132-7. This definition states that this is a system comprising camera points, control units and devices for transmission and control; the system may be indispensable for surveillance of the specific security zone. According to a definition from the cited standard, the camera is a device that contains image intensifier, which generates a video signal from optical image [13]. The author is of the opinion that all the presented definitions of video monitoring describe the essence of its functioning in a broad and general way.

2. Video monitoring versus standardisation regulations

Video monitoring, which is an element of the public security and order system, should be functioning based on installations (devices and software) used for reception, recording of images, recording and their playback. The entire CCTV system should guarantee that the assumed goals would be implemented and that the operating effectiveness would be as required. What is more, it should be constantly evaluated. To be able to make full use of possibilities allowed by video surveillance systems, they require adaptation to principles specified in standardisation regulations. Until 2016 the binding Polish standard related to alarm systems was CCTV surveillance systems used in protection measures – Part 7: Guidelines for application (PN-EN50132-7:2012-04). The standard defined procedures connected with designing systems and technical parameters of the equipment being used depending on the defined goal. It extended regulations as compared to the preceding standard (PN-EN 50132-7:2003) by IP technologies, introduced issues of protection from access to devices in the physical dimension, and also allowed for issues of system integration [14]. Among others, on the basis of those standards the Katowicki Inteligentny System Monitoringu i Analiz (the Katowice Intelligent Monitoring and Analyses System) has been built. As of 2016 a new standard came into effect:

PN-EN 62676-1-1: 2014-06 CCTV Surveillance systems used in security. Part 1-1: system requirements – General provisions [15]. The IEC standard *(International Electrotechnical Commission)* introduced among others a new term, and namely VSS (*Video Surveillance Systems*) used alternatively with CCTV. The standard defines minimum performance and functional requirements which have to be agreed in relations between the user, the law and the supplier. Similarly as in the case of the preceding standard it does not regulate requirements pertaining to designing, planning, testing, operation or maintenance. The standard refers to systems of remotely monitoring sensors, which activate the CCTV systems. The standard PN-EN 62676-1-1:2014-06 is applicable in VSS systems that distinguish means of detection, release, mutual connections, control, communication and network powering with other applications. Specific requirements with respect to usage of applications for the recognition and detection are contained in guidelines of IEC 62676-4. The classification of particular recognition and detection applications describes the objective of using CCTV, and concurrently determines standards with respect to the degree at which the screen is filled by a human silhouette. Particular applications are described by Z. Szachnitowski who stipulates that 5% of screen filling is required from the monitoring application, and as regards inspection the standard defines the screen filling scale of 400% of the fragment of a person being identified. Such application is most desires in case of identification or evidence related studies [16, p. 38]. The new standard was published on 2 September 2014 and has imposed the deadline for adaptation of new standards by 2 December 2016. Standardisation guidelines regulate the following issues:

- legal basis, terminology, definitions and abbreviations;
- rules for the organisation of systems, including: general regulations pertaining to VSS, specific regulations concerning recording and processing of video material;
- principles for system management, including: data management, organisation management, cooperation with other systems;
- system security, including: integrity of the system, integrity of data, protection levels;
- technical requirements, including: requirements related to the recording of images, their processing and image quality;
- definition of space in which the images are recorded;
- rules for documenting operation of the system.

The guidelines depict three spheres which are determinants for the effective use of VSS systems, and namely: environment of picture recording, system management and system security. As regards the image recording surroundings, the main dimensions for effective functioning of CCTV systems comprise recording of the incident, processing the footage, displaying it to an operator along with associated information for easy and effective usage. In the sphere of "System management" the standard distinguishes issues pertaining to the management of data and actions and cooperation with other systems. As regards cooperation with other systems the standard indicates that particular data formats have to be harmonised for all systems. The guidelines indicate the following as examples of cooperating systems:

- other security systems (e.g. intrusion alarms, panic alarms, fire protection alarms);
- other security management systems (e.g. management centres);
- other systems not directly connected with security (e.g. ATMs, recognition systems of registration plates, building management systems, recording systems in commercial premises).

In the sphere of "System security" the standard distinguishes two categories, i.e.:

- integrity of system – understood as physical protection of system elements, access control to the system (physical protection of cameras and of access to video system);
- integrity of data – understood as securing access to data, rendering the loss of data impossible and impeding any modifications (manipulations) of recorded footage.

The guidelines describe the security policy related to the risk of occurrence of specific hazards and accidents in relation to possible consequences of the occurrence of such situations. Moreover they introduce a four-level security and risk management system.

The standard PN-EN 62676-1-1:2014-06 attaches considerable importance to data storage methods, especially in the context of their possible loss. This points to the necessity of fulfilling several technical requirements related to image quality, such as resolution and size of stored pictures, picture compression methods, determination of the time of repeated recording after system re-boot. Pursuant to the guidelines the monitoring system should among others provide on-going information on:

- volume of recorded footage;
- ability of storing the recorded footage;
- time of recording;
- remaining free memory that allows recording.

The guidelines define general rules for data archiving and indicate that they have to be stored for evidence purposes. On the other hand, there must be a possibility of their transmission or playing at another location. There must also be technical possibilities allowing continuous recording of the system, also at the time when the recorded footage is played back. Using data compression the standard recommends that no use is made of software that requires the manufacturer's consent to its usage. The standards refers to format in which data may be recorded. It also provides example of the recommended formats constituting international standards such as:

1. formats of video recordings:
- H.264: AVC: ISO/IEC 14496-10;
- MPEG-4 part 2: ISO/IEC 14496-2;
- MPEG-2: ISO/IEC 13818-1;
- H.263: ITU-T Rec. H. 263;
- JPEG 2000: ISO/IEC 15444-1;
- JPEG: ISO/IEC 10918-1.

2. formats of audio recordings:
- G. 711: ITU-T Rec. G.711;
- G.726: ITU-T Rec. G.726;
- AAC. ISO/IEC 14496-3.

3. data export, file format:
- MP4: ISO/IEC 14496-14;
- MPEG-A: ISO/IEC 23000-10:2009.

The discussed guidelines specify principles to be adopted during the transmission and footage playback, i.e.:

- it is not admissible to change the quality of the footage, its resolution, and during data export not loss should take place of particular footage pictures;
- the system should not apply further compression or conversion of exported data – this could reduce their usability;
- if possible, along with the recording also authorised signatures and metadata should be sent;
- the system may not lose its basic functionality during the data transmission;
- the expert method should be appropriate for system capabilities.

The standard specifies requirements for the programme for playback of footage which should have the following functions:

- real time play;
- stop, pause, forwards and background winding and playing "frame after frame", as well as reverse playing;
- watching the view from one or more cameras, concurrently maintaining the adequate ratio of frame size;

- showing the image from one camera with the maximum recording resolution;
- possibility of searching the footage contents, in line with the adopted time criterion;
- possibility of recording footage, and its later printing with specified time and date of recording;
- possibility of synchronising images from a few cameras at the same time;
- possibility of playing back audio files and other metadata;
- ability of transmitting images in standard formats;
- the system should show the time, date and other information related to the footage in a legible way.

A key requirement posed for system administrator is the usage of software that enables playback of recorded footage on computers having the Windows operating system.

Further guidelines pertain to areas connected with management, i.e. "System management" and "management of actions, operations". As regards management of the system, authors of the standard indicate inter alia the following requirements:

- handling of the system has to be simple, quick and intuitive to the user;
- legible information has to be provided continuously as to the state of system operation;
- the system must identify without delay alarm situations including information concerning the event (the information has to be concise and legible).

As regards management of specific activities, the standard refers in particular to systems that use intelligent components of image analysis. It imposes among others the following requirements:

- alarm data (alerts) must have priority over data recorded automatically in a continuous mode;
- picture viewed by the operator have to be clearly described as footage either being watched live or replayed;
- a very important requirement concerning providing information whether the footage had been recorded automatically (triggered by the alert), or in the manual mode (at the operator's instructions);
- footage from alert recording has to be available in the same sequence at which they had been recorded. The only exception are situations in which a gradation of priorities takes place. In such a case priority alerts have priority over the remaining ones;
- the system has to use clearly different signals for diverse situations: alerts, system breakdowns or attempts at manipulating of the system;

- the alert has to be visible for the operator (image) and audible (sound). As regards an alert concerning an event classified as security level 3 and 4, the system should provide additional information (source of alert, type of alert, date, time);
- the system administrator should carry a log.

The guidelines specify which activities have to be documented depending on the security level, e.g.:

- starting of alarm – at levels within the range of 2–4;
- manipulations in the system – at levels within the range of 3–4;
- loss of recordings or restoration of video recordings – at levels within the range of 3–4;
- loss of power supply – at levels within the range of 2–4;
- reactivation of the system (system reset), its stopping – at levels within the range of 2–4;
- searching for recordings and their playing– at levels within the range of 3–4;
- change of recording parameters – at levels within the range of 3–4.

The scope related with security of the system comprises: integrity of the system and data integrity. Worthy of attention are regulations concerning the ascertaining of defects, where similarly as in the event of alerts defects should be graded. Furthermore, the system should also enable continuous recording of footage. The recorded footage may not be lost in the event of a power failure. Pursuant to the standard the system should automatically detect and alert of attempts at manipulation of footing. Examples of such manipulations include: modification of data during processing of footage, deletion of the footage, blurring or deformation of the image, change of the field of the camera's view. Each work carried out on the recorded footage needs to be authorised by using fingerprints, a digital watermark or the use of a cryptographic algorithm with the use of a control amount.

Worthy of attention is a definition of space under surveillance. The standard divides that space into the following four classes:

- Class I – interiors of a residential or commercial building within a range of temperatures: from –5°C to +40°C and moisture of ca. 75%;
- Class II – interior of a building where no constant temperature is maintained (corridors, basements, storage areas), within the temperature range from –10°C to +40°C, at a 75% moisture;
- Class III – outside, where components of the system are not exposed to direct impact of rain or sun, potentially extreme conditions inside the building, within

the temperature range from –25°C do +50°C, at humidity of 75%, and for 30 days within the range of 85–95%;

- Class IV – outside, where components of the system are fully exposed to weather conditions, within the temperature range from –25°C to +60°C , at humidity of 75%, and for 30 days within the range of 85–95%.

As to documenting activities connected with handling of the system, the standard indicates that the documentation should be concise, clear, complete, and sufficient for system installation, its start, functioning and sustaining its operation.

To recapitulate, the analysed standard PN-EN 62676-1-1 provides a specific outline of requirements for the effective and safe usage of video monitoring systems. There is also a reference to systems that make use of modern applications for picture analysis, which are based on generating alerts, as well as a reference to the safety of IT data. Planning and building of modern urban monitoring systems has to be carried out pursuant to international technical standards. The investor should clearly define to the contractor the obligation of creating the system according to relevant binding standards. An example of such a standpoint is the establishing of the Katowicki Inteligentny System Monitoringu i Analiz. At this point it should be emphasises that the adoption of the standards is of voluntary nature in accordance with contents of art. 4 item 3 of the act of 12 September 2002 *on standardisation*, which indicates that in national standardisation use is made inter alia of the voluntary principle of participation in the process of standard development and application [17].

3. Closed-circuit television – perspectives

Considering how popular closed-circuit television systems are around the world, dynamic development of this technology can also be expected in Poland. In 2016, the CCTV market recorded a smaller increase in sales, mostly due to suppliers from China who aimed at lowering prices and increasing their market share. It is interesting to note that western CCTV specialists did not respond with price cuts or margin reductions to the aggressive policy of Chinese suppliers. Their actions were rather directed at investing in new technologies and solutions with advanced software for data analysis. Those solutions were intended to ensure a greater return on investment for users, a lower total cost of maintenance, and higher quality business analytics. According to specialists, in 2017 the CCTV market was no longer perceived just as a personal and property security market, for instance because it employed age and gender analysis, and facial recognition algorithms in the retail sector. These algorithms made it possible to adjust advertising content to match the age and sex of a person within range. Other examples include the use of face recognition technology for automatic registration of lectures at universities, or the use of 360-degree cameras in tourism to count and track the movement patterns of people in stores, hotels and resorts to aid the streamlining of business operations [18].

Enhancement of the monitoring system, and in particular its combination with software for the analysis of images transmitted to the receiving centre, offers a wide range of opportunities. It is one of the main directions in which the CCTV networks supported by appropriate software are being developed. Our current experience could indicate problems related to the correctness and reliability of video image analytics. Therefore, it may seem that the networks are failing to fulfil our hopes. However, recent years have shown significant changes leading to an improvement in both algorithms and software, which use, among others, a machine learning technique known as deep learning. A definition of machine learning offered by P. Cichosz states that "[…] a system learns with every autonomic change to the system that is made based on experience and leads to the improvement of its functioning [19, p. 34]. The author also points out that machine learning is among the most significant fields of artificial intelligence. AI is perceived as a field of research that is aimed at producing intelligently operating computer programs. Learning systems are directly connected with two other sections of AI, i.e. automatic reasoning and heuristic searching. Automatic reasoning is the oldest stream of artificial intelligence based on the achievements of formal logic, which strives to obtain effective deduction algorithms. An effective search of large spaces is of interest for artificial intelligence due to its two applications: problem solving and board games [19, p. 50]. Automatic reasoning is the direction of AI development that finds application in the development of closed-circuit television, including urban surveillance systems. This mostly refers to the elements of intelligent image analysis combined with the generation of alerts, including a reduction in the number of false positives. On the other hand, reasoning-based machine learning can develop possibilities allowing the prediction of certain events or types of behaviour. In this case, learning is a result of two processes: reasoning, which leads to the generation of knowledge; and recording, which allows new knowledge to be stored in the system's memory in accordance with the adopted representation method [19, p. 53]. The application employed the *deep learning* method to analyse the *Suspect Search* image and, among other things, within a few seconds determine the location of a person within the CCTV perimeter [18, p. 20]. One of the first advanced solutions used in closed-circuit television was the ANPR *(Automatic Number Plate Recognition*) system. The system (which was originally used in Great Britain) registers and automatically identifies number plates, drivers and passengers of vehicles that drive by. When a wanted vehicle is identified, an alarm is raised. London's ANPR system, which was expanded in the 1950s, is capable of analysing 5,000 plates per minute. The system allows the identification of the plate numbers of a vehicle moving at a speed of 200 km/h and is 98% effective [5, p. 49]. As reported by the Panoptykon Foundation, the authorities of 21% of Polish cities declared that their monitoring systems feature ANPR [9, p. 17].

Another solution that is implemented on a large scale is VCA, i.e. the *Video Content Analysis* system, which, generally speaking, allows the identification of "suspicious behaviour" [20, p. 29]. The basic functions of intelligent content analysis are as follows:

- sabotage detection;
- intelligent detection of movement (suspicious behaviour);
- zone detection (an alarm is triggered by movement in a specific zone);
- number plate recognition;
- head count;
- line crossing detection (e.g. when the safety line is crossed at a train station platform);
- object tracking;
- audio detection (when a certain loudness threshold is exceeded);
- smoke and fire detection;
- facial recognition [21].

VCA is gaining popularity as a service in the field of development and the use of CCTV systems. This fact is proven by, for example, the large quantity of service offers available online [22, 23]. This type of a solution was employed by the creators of the Katowice Intelligent System for Monitoring and Analysis. Alongside the city monitoring system in Zielona Góra, it is considered to be one of the most modern systems in Poland. Its wonder is rooted in the application of specialised, advanced software. The system uses the following components:

- a licence plate recognition (LPR) system (*Milestone*). The system is installed at 10 road locations on the main road routes in Katowice;
- the IBM IVA (*Intelligent Video Analytics*) system – a component of the installed video analytics. Selected cameras in the Katowice Intelligent System for Monitoring and

Analysis have analytics configured to identify the following situations: a person lying down, an abandoned object, a removed object, a gathering, zone crossing, forcible entry to a vehicle, wrong-way driving, parking, vehicle collision, the appearance of animals in a zone, vandalism, a shift in the location of an object. The alerts generated by analytics are displayed on the operator's screen;

- the IBM IOC (*Intelligent Operations Center*) application – an operating system enabling the operators to use the IBM IVA component. The application verifies whether a given alert is true and forwards the signalled incident to the services for handling, etc.

The software allows automatic documentation of the system operators' work through:

- automatic generation of reports on, for example, the number of alarms, types of alarms, etc.;
- automatic generation of system logs (among others: logging into the system, time of handling a given camera, time and scope of exported video content, video content blockages);
- automatic registration of interventions conducted by services based on events recorded via CCTV.

New capabilities of CCTV systems were among the topics subject to research and development under the INDECT project, i.e. the intelligent information system supporting observation, searching and detection for security of citizens in urban environment. It was an international research project intended to employ innovative algorithms and IT methods to detect and combat terrorism and other criminal activity. The project was financed by the European Union. INDECT's aim was to create a set of solutions for intelligent observation and automatic detection of suspicious behaviour or violence in the urban environment. The project was partnered by Polish universities, i.e. the AGH University of Science and Technology in Kraków, Gdańsk University of Technology and Poznań University of Technology [24]. Works under the project commenced on 1 January 2009. As of the very beginning, the project was intended to involve research to increase the security of citizens and protect the recorded and stored information. This regarded the use of innovative methods to detect physical threats by using intelligent surveillance systems, and threats in the virtual world, i.e. in computer networks and online. With regard to detailed objectives related to closed-circuit television, the INDECT project assumed the creation of an intelligent multimedia information processing system for the automatic detection of threats and identification of criminal activity or violence. Moreover, the project was expected to develop intelligent video and audio data analysis in order to detect threats in urban areas [25, p. 27]. The literature lacks specific information on the implementation of the INDECT project. There is also no information on the results of the team's work. However, there are some indications of concerns regarding the functioning of the INDECT system. Its technological layer is particularly interesting, as the system does not create any new surveillance tools. Instead, it uses the existing video surveillance systems – its novelty is not the means of surveillance but the way in which already available means of surveillance are used. The optional use of private users' cameras, cameras in stores and at petrol stations, etc. that would be connected in one network is also indicated. The development of algorithms, as a part of the project, that allow an on-going analysis of images recorded by cameras to detect behaviour that could indicate the intention to commit a crime seems exceptionally futuristic [26]. As stated above, it is an element of reasoning-based machine learning. An example of behaviour detection would be the case of a paedophile who can be identified on the basis of behaviour characteristic of this type of criminal. If the system identifies such behaviour, it will notify the operator or another person. The identification itself will not have any legal effects, and the ultimate decision as to interpretation and further actions will be taken by a human being. Similar procedures based on revealing criminal intent are employed by law enforcement authorities in the science-fiction film "Minority Report" [27]. The Ministry of the Interior was one of the project's partners, but in 2012 a decision was made to suspend the cooperation of the Police with regard to the INDECT project. The decision was made by the Minister after consultations with the Police Commander-in-Chief. As it was explained, the Police already possessed means that allow the prevention of threats to public order [28]. According to the scientists at the AGH University of Science and Technology, the distrustfulness towards INDECT was a result of the protest against ACTA that was happening at that time. INDECT and ACTA had nothing in common, but society was very sensitive to all things related to the public services' activity, especially online. This theory was supported by publicists. D. Maciejasz claimed that the Ministry most probably got frightened by the wave of protests to which people were incited online in the weeks prior by comparing INDECT to ACTA. Further, she quoted B. Bubula, a member of the Sejm, who referred to INDECT as an "Orwellian system of great surveillance" [29, p. 3]. The discussion on the decision taken by the Ministry of the Interior invoked the conciseness of the message, which lacked any exhaustive justification [30]. Further, it was pointed out that foreign entities, including Europol, the Spanish Ministry of Defence as well as the Latvian, Romanian, Maltese and Czech Police were interested in purchasing the INDECT system [29, p. 3].

Another project related to enhancing video image analyses is COPCAMS, in which participated technical universities and research institutes from France, Spain, Turkey, Denmark, Slovenia, Great Britain and Poland. 25 partners participated in it in the years 2013–2016, including the Gdańsk University of Technology. The project was co-financed by the National Centre for Research and Development and the EU initiative ARTEMIS. The name of the project, COPCAMS, is an abbreviation for Cognitive and Perceptive CAMeraS. The research concerned the working out and testing of new intelligent solutions for industrial cameras, closed circuit TV system, video diagnostics on production lines and other areas where video analytics are used [31, p. 20]. Under the project the Gdańsk University of Technology coordinated the execution of tasks under the package "Advanced concepts for camera systems", which was dedicated to new methods of processing video footage and multimodal data, i.e. those coming from additional various types of sensors and from compression of video signals and data transmission. The first innovative solution in this respect was the development of an acoustic radar integrated with a rotating camera. Its task is to carry out live analyses about the vector gradient of acoustic pressure, from which information may be obtained about the situation of sound sources in the entire space surrounding the camera. In this case the utilisation of an appropriate software for the detection and locating sources of sounds, of importance from the viewpoint of security, is able to detect and direct the rotating camera towards the source of the scream, explosion, shot or sound of broken glass. The source classification algorithm has been developed on the basis of real recordings and distinguishes their classes. As an effect it does not respond to typical sounds, such as road traffic noise or conversations. The number of events to which a camera might react is unlimited, and their scale and types depend on the operator (the operator may set the system on the closest source, the loudest source or whether the highest priority should be assigned to a scream, a broken window, or a shot). The next solution proposed by researchers from the Gdańsk University of Technology was the development of multisectoral directional antenna for the detection and location of active radio markers executed in the RFID technology. Such markers are used to secure goods in the shops and are activated at the time of passing through narrow gates serving as transmitting and receiving antennas. As a rule those markers operate in the passive version (without incorporated battery). The scientists have made use of the active version of the marker and a directional antenna, which allows continuous surveillance of the presence and location of the protected item. Project participants have proven that it is particularly interesting and desirable to streamline movement detection and object monitoring methods. In the currently used "intelligent" systems, devices furnished with low-effectiveness processors, much too frequently false alarms are generated, such as for example rippling of leaves, water, reflections. The basic operation performed on each image pixel is modelling the background in a way that would allow adaptation to:

- slow changes in the picture, e.g. clouding that changes the brightness and colours of the entire frame cannot be interpreted as movement;
- quick cyclical changes in the image, such as for example movements of leaves causing alternating changes of green colour (leaves) to blue (sky), in cases when this should be interpreted as background of the image and not movement.

Consequently it is necessary to apply highly effective processors which might carry out the required calculations[1]. Results of research of the remaining partners of the COPCAMS project appeared to be interesting and promising. We can specify the following examples of research works which can be applied in the implementation of tasks related with public safety and order:

- combination of possibilities of acoustic and radio surveillance with video monitoring to enhance the possibilities of effective and precise detection and observation of events;
- development of cooperation methods between algorithms controlling wide-angle lens cameras and rotating cameras to watch over a vast area;
- streamlining methods aimed at improving picture legibility in the event of fogging or under – exposure.

In the European Union member states intelligent invigilation will most probably be taking place on a mass scale, because the European Commission earmarked in 2004 over EUR 60 million on preliminary research, which is to allow devising of a system called ISCA PS (*Integrated Surveillance of Crowded Areas for Public Safety*). It is to make use of all new tools of intelligent invigilation, inter alia the technique of electronic conversation tapping by automatic lip reading, on the development of which scientists from the British Surrey University are currently working [25, p. 25–26].

[1] A 1 Mpix video frame requires calculating and updating 24 times a second a milion pixels in the background module. Source: [31].

As suggested by specialists, in 2017 one of the main dimensions of interest in the event of CCTV is cybercrimes. This was related to a DDoS attack, which took place at the beginning of 2016. The concept of DDoS comes from the English term *distributed denial of service*. This is one of many methods used to block Internet services or block Internet connections. There are two basic types of DDoS attacks, i.e.:

- volumetric attack – in which mass amounts of unwanted data are sent to the indicated IP address, which as an effect causes blocking or slowing down of the Internet link;
- application attack – in which IT resources of the Internet application are exhausted, e.g. calculating power or memory [32].

The DDoS attack of 2016 on a US company that manage servers caused among others suspension of services of Amazon and Netflix. During this attack use was made of remotely controlled "attackers" called bots, and in addition a few network cameras and system recorders infected by the Miari malware. This incident has once again pointed to the need of assuring appropriate protection of devices and IP systems.

Another development direction for the technology of video monitoring is the adoption for this purpose of unmanned aircraft, the so-called drones. Unmanned aerial vehicles are automatic flying devices with their own propulsion, which may fly in the air on their own. They may also be remote controlled, and depending on the equipping may serve diverse needs [33, p. 119]. Rules for the use of drones are regulated to a certain extent by provisions of the act of 3 July 2002 *The Aviation Law* [34]. Apart from the fact of using drones in air space and the ensuring problems in air transport, they may also be used as platforms that carry cameras. Consequently they might prove to be suitable for implementation of tasks which up to now were difficult, and in some cases hazardous or costly. Such tasks comprise responding to natural calamities, border control, demonstration control and combatting cybercrimes. In Poland apart from the military forces drones are also used by the police and the fire service. They are also commonly used by private citizens. Currently in Poland there are ca. 100 000 drone owners – only nine times fewer than users in the United States, which places us on the top global position. In 2015 revenues from the sale of unmanned aerial vehicles came up to PLN 164 million, and only a year later exceeded PLN 200 million, and a year ago have reached the level of PLN 250 000 000 [35, p. 8]. Drones keep giving rise to controversies mainly due to the large scale of interference with our privacy. They may be used to observe people and vehicles and to watch private space. Such monitoring may be implemented in a way that is practically imperceptible for the persons being surveyed.

As regards the future of CCTV systems, an interesting opinion has been presented by U. Segall – director for business development in the Israeli company called Qognify. He refers to the usage of posts and videos published from devices of the users in social media. He suggests that some technologies allow compilation of posts from social media and the integration of those data. The amount of data associated with the possibility of locating the user and the time of recording may prove to be of importance as regards of protecting people and property. Consequently in his opinion the best lens and the most intelligent "detector" is still man. When using smartphones (equipped with GPS, advanced video systems and communication tools), the users can record and transmit a large amount of data suitable with respect to safety and order [18, p. 18].

Summary

Video monitoring systems are currently commonly used as tools aimed at assuring public security and order. The effective functioning of CCTV systems requires adaptation to binding international technological standards that regulate their structure and operation. The binding standard PN-EN 62676-1-1 presents in great detail requirements related to effective and safe usage of video monitoring systems. The standard refers to systems that make use of modern applications for image analyses, based on the generation of alerts. It associates considerable important to security of video recordings, both from the IT and physical viewpoint. This is of a great importance in the context of usage of obtained materials by the law enforcement authorities and justice system. The creation and usage of video monitoring systems pursuant to the binding standards provides a partial guarantee of effective and safe operation. Based on European technical standards among others created was the Katowicki Inteligentny System Monitoringu i Analiz (Intelligent System of Monitoring and Analysis in Katowice).

Technological development offers possibilities to video monitoring systems which earlier on remained solely in the imagination of authors of science fiction movies. Those possibilities arise mainly from dynamic development of the IT industry. The currently built systems already make use of tools that allow "intelligent" observation of the monitored area. They are mostly based on a video and acoustic analysis of the observed reality. They generate alerts if any anomaly is detected, automatically review the images being recorded and respond to the events in an automatic way. All those options assist or even take over on-going analyses of recorded footage from system operators. All the same it is still the human being who has to interpret the meaning of the recorded footage and to take further decisions accordingly.

It should be emphasised that "intelligent" systems are not free of defects. One of the problems is the generation of "false alerts". Alarms may be caused by insignificant changes in the reality being observed (e.g. leaves on trees moved by the wind, light reflexes). For this reason one of the development directions of software that controls systems of video monitoring systems is work on machine learning, which is now considered one of the most important spheres of artificial intelligence. This will allow making automatic and correct interpretations of the analysed footage.

Work on artificial intelligence that supports the operation of video monitoring is one of the main directions for technological development. Other directions concern possibilities of the use of different types of cameras that observe reality. The concept relates to the possibility of access to all classical camera points, as well as cameras installed in smartphones handled by private users or cameras installed on drones. It is characteristic that the development of technology is not determined only by the possibility of usage by public entities (e.g. to enhance public security and order). Also not be to underestimated is the pressure coming from the private sector. One of the possible examples may be the advertising sector where video surveillance systems are capable of automatic recognition of the gender or age of a person and in such a way make the best choice of advertisement contents. The needs of both the public and the private sectors consequently assure a guarantee that works on the development of CCTV systems would be further continued.

References

[1] Spencer A.R, *Psychologia współczesna*, Gdańskie Wydawnictwo Psychologiczne, Gdańsk 2004.

[2] Wiśniewski B., *Bezpieczeństwo wewnętrzne państwa – pojęcie, istota, system, konteksty* [w] *Od nauk wojskowych do nauk o bezpieczeństwie,* B. Wiśniewski (ed.), Wyższa Szkoła Policji w Szczytnie, Szczytno 2014.

[3] Wiśniewski B., *System bezpieczeństwa państwa. Konteksty teoretyczne i praktyczne,* Wyższa Szkoła Policji w Szczytnie, Szczytno 2013.

[4] Wróblewski M., *Podstawy prawne funkcjonowania monitoringu wizyjnego w Polsce,* "Monitor Prawny" 2013, No. 8.

[5] Waszkiewicz P., *Wielki Brat Rok 2010. System monitoringu wizyjnego – aspekty kryminalistyczne, kryminologiczne i prawne,* Wolters Kluwer, Warsaw 2011.

[6] www.PreciseSecurity.com (download: 15.01.2020).

[7] Informacja o wynikach kontroli Najwyższej Izby Kontroli *Funkcjonowanie miejskiego monitoringu wizyjnego,* https://www.nik.gov.pl/plik/id.6400.vp.8169.pdf (download: 14.11.2019).

[8] M. Szumańska, *Życie wśród kamer. Przewodnik,* Fundacja Panoptykon. http://zycie – wśród – kamer. panoptykon. org/ (download: 06.11.2019).

[9] Krassowski K., *Monitoring wizyjny z punktu widzenia kryminalistyki* [in:] *Prawo Kryminalistyka Policja. Księga pamiątkowa ofiarowana prof. B. Młodziejowskiemu,* (ed.) J. Kasprzak, J. Bryk, Wyższa Szkoła Policji w Szczytnie, Szczytno 2008.

[10] Dunaj B., *Słownik współczesnego języka polskiego*, Przegląd Reader's Digest, Warsaw 2001.

[11] Kałużny P., *Telewizyjne systemy dozorowe,* Wydawnictwa Komunikacji i Łączności, Warsaw 2008.

[12] Ordysińska M., *Aspekty prawne funkcjonowania systemów monitoringu wizyjnego w Polsce. Cz. I.,* "Systemy Alarmowe" 2006, No. 4

[13] Wittich P., *Instalacja kamer to za mało, żeby zbudować skuteczny system monitoringu wizyjnego,* "Kwartalnik Policyjny" 2016, No. 1 (36).

[14] http://www.sa-portal.pl/nowosci/samsung-techwin-i-mr-system-sponsorami--projektu-polskiej-normy – prpn-en-50132-72012/ (download: 10.12.2019).

[15] Standard PN-EN 62676-1-1 available at https://czytelnia.pkn.pl/#/reading-room/PN – EN%2062676-1-1:2014-06E/~/PN-EN%2062676-1-1_2014-06E_ KOLOR.pdf/1 (download: 04.11.2019).

[16] Szachnitowski Z., *Systemy dozorowe CCTV i ich przydatność dowodowo –wykrywcza,* "Ochrona mienia i informacji. Projekty, instalacje, zarządzanie" 2014, No. 2.

[17] Act of 12 September 2002 *on standardisation* (i.e. Polish Journal of Laws/ Dz.U. from 2015 item 1483).

[18] Pao W., *Telewizja dozorowa. Światowe trendy 2017*, "A&S Polska" 2017, No. 2.

[19] Cichosz P., *Systemy uczące się,* Wydawnictwa Naukowo-Techniczne, Warsaw 2007.

[20] Mroczek A., *Rejestracja obrazu w miejscach publicznych,* "Ochrona Mienia i Informacji" 2013, No. 3.

[21] VCA-inteligentna analiza obrazu. http://www.tvprzemyslowa.pl/vca-inteligentna--analiza-obrazu-3/ (download: 17.12.2019).

[22] http://www.wimax.pl/inteligentna_analiza_wideo-s121.html (download: 17.12.2019).

[23] http://www.ismeurocenter.com/ismeurocenter.pl/produkty/cctv/vca-analiza--zawartoci-obrazu (download: 17.12.2019).

[24] http://www.kt.agh.edu.pl/pl/projekt/281 (download: 12.12.2019).

[25] Wróbel J., Podsiedlik P., *Monitoring wizyjny cz. I. Geneza i czasy współczesne.* Materiały Dydaktyczne nr 37, Szkoła Policji w Katowicach, Katowice 2016.

[26] Michalik Ł., *Projekt INDECT – AGH tworzy narzędzie masowej inwigilacji?* http://www.gadzetomania.pl/6611,projekt-indect-agh-tworzy-narzedzie-masowej--inwigilacji#comments (download: 12.12.2019).

[27] Spilberg S. (dir.) , *The Minority Report*, 20th Century Fox (distr.), 2002.

[28] Communication on the INDECT system of 13 April 2012 www.mswia.gov.pl /pl/aktualności /9729,dok.html (download: 12.12.2019).

[29] Maciejasz D., *AGH już dziękujemy,* "Gazeta Wyborcza" 2012, No. 88.

[30] Wasilewska – Śpioch A., *MWS wycofuje się z projektu INDECT*, 14.04.2012, http://www://di.com.pl/msw-wycofuje-sie-z-projektu-indect-44743#dalej (download: 12.12.2019).

[31] Szczuko P., *Nie tylko kamery. Tematyka i wyniki badań projektu COPCAMS,* "A&S Polska" 2017, No. 2.

[32] *Co to jest atak DDos i jak się przed nim chronić*? https://dataspace.pl/assets/ddos_broszura_web.pdf (download: 06.12.2019).

[33] Lis S., *Bezpieczeństwo a bezzałogowe statki powietrzne (drony) w działaniach militarno-wojskowych i w służbie cywilnej* [in:] *Bezpieczeństwo w kontekście zglobalizowanego* świata (ed.) P. Maciaszczyk, Państwowa Wyższa Szkoła Zawodowa im. prof. Stanisława Tarnowskiego w Tarnobrzegu Tarnobrzeg 2017.

[34] Act of 3 July 2002 *The Aviation Law* (Polish Journal of Laws/Dz.U from 2018 item 1183, 1629, 1637).

[35] Wojciechowski K., *Oblatani w dronach,* "Dziennik Gazeta Prawna" 2018, No.155.

Grzegorz Matuszek – Graduated from the Police Academy in Szczytno. Doctor of social sciences in the discipline of security science. Teaching employee at the WSB Academy in Dąbrowa Górnicza. First Deputy Commander of the Poviat Police in Wodzisław Śląski.

---

dr Grzegorz Matuszek – absolwent Wyższej Szkoły Policji w Szczytnie. Doktor nauk społecznych w dyscyplinie nauk o bezpieczeństwie. Pracownik dydaktyczny Akademii WSB w Dąbrowie Górniczej. Pierwszy Zastępca Komendanta Powiatowego Policji w Wodzisławiu Śląskim.